IoT 네트워크에서 개인정보 보호를 위한 블록체인 기반의 안전한 다자간 계산 아키텍처

진호천*, 박희지*, 박종혁*
*서울과학기술대학교 컴퓨터공학과
{chahot, heeji, jhpark1}@seoultech.ac.kr

Blockchain-based Secure Multi-Party Computation Architecture for Privacy Preserving in IoT Network

Haotian Chen*, Heeji Park*, Jong Hyuk Park*
*Dept. of Computer Science, Seoul National University of Science and Technology

요 약

IoT 장치들은 연구, 의료, 금융, 민생 분야 등에 지원하고 있으며 취약한 보안 메커니즘으로 인하여 IoT 네트워크의 개인정보 안전성이 중요해지고 있다. 안전한 다자간 계산은 서로 믿지 않는 참여자라도 데이터 수요자에게 원본 데이터를 누설하지 않는 범위 안에서 다자간 연합 계산 능력을 제공한다. 상업 네트워크나 산업 네트워크에서는 대량의 데이터는 다른 플랫폼들과 통신하기 때문에 기업이나 개인의 개인정보 데이터가 통신 과정에서 도청될 경우 데이터 보유자에게 막대한 경제적이나 잠재적인 손실이 발생한다. 본 논문에서 데이터 통신 과정을 계층별로 정의하여 블록체인에 기반의 안전한 다자간 계산 아키텍처를 제안한다. 제안하는 이키텍처에서 블록체인을 사용함으로써 데이터의 유효성 및 검증 가능성을 보장한다. 인증된 데이터로 안전한 다자간 계산 수행하기 때문에 통신 과정의 보안성 및 기밀성도 확보한다. 암호학 및 블록체인 기술의 지속적 발전 및 활성화에 따라 제안하는 아키텍처가 지속적으로 개선할 잠재력이 있다.

1. 서론

무선 통신 기술 및 정보처리 기술의 지속적인 발전에 따라 네트워크 중의 데이터 통신 트래픽이 점차 증가하고 있다. 사물인터넷(IoT)은 이질적인 장치들을 통해서 여러 지역에서 데이터를 수집하는 네트워크이다 [1]. IoT 환경에서 수집된 수많은 데이터가 인정되지 않으면 유효성을 보장할 수 없다. 유효하지 않은 데이터는 악의적인 의도로 네트워크에 보내는 확률이 높기 때문에 안전한 네트워크 환경 구축하기 위해서 인증 메커니즘은 필수적이다 [2]. 블록체인은 공평하고 합의 알고리즘을 이용하여 인증 메커니즘을 제공하기 때문에 부인방지 및 신분식별이 가능하다. 블록체인은 주목받고 있는 인증 기술 중 하나이다.

인증된 노드라도 그들이 제공하는 데이터는 개인의 이익이나 단순한 악의에 의해 다른 노드의 정보를 악의적으로 이용할 수 있다. 뿐만 아니라 산업화 네트워크에서 상대방이 악성 의도가 없더라도 어떤 민감한 데이터 자체가 기밀성에 대해 강한 요구되어서 외부 노출하면 안 된다 [3]. 안전한 다자간 계산은 참가자 자신의 개인 입력을 드러내지 않고 분산 네트워크에서 참가자가 공통의 목표에 대해 각각의 입력에 의존하는 공동 계산을 할 수 있도록 하는 기술이다 [4]. 안전한 다자간 계산는 최근 몇 년간 클라우드 컴퓨팅, 지능형 컴퓨팅, 엣지 컴퓨팅 등의 기술이 보편화되면서 열기가 상승했다. 안전한 다자간 계산은 개인 데이터 컴퓨팅을 위한 범용 도구로서 다자간 계산 분야의 개인정보 문제를 해결하는 데 자연스러운 장점을 가지고 있다.

본 논문에서 블록체인 및 안전한 다자간 계산에 대한 보안 우월성을 조사하고, 기존 연구를 바탕으로 IoT 네트워크에서 발생하는 특정한 개인정보 보안 문제에 대해 고찰한다. IoT 네트워크 특정에 맞은 아키텍처를 제안하고 블록체인 및 안전한 다자간 계산을 연동하는 이론을 서술한다. 마지막으로 제안하는 아키텍처에 대해 지속적 발전 가능한 이점을 제시한다.

2. 관련연구

본 절에서는 IoT 네트워크에 존재하는 개인정보 위협을 설명하고 및 기술 동향을 서술한다.

2.1. IoT 네트워크에 존재하는 개인정보 위협

IoT 네트워크에는 방대한 양의 데이터가 존재하며, 이런 데이터는 모두 IoT 장치의 센서에서 수집된다. IoT 장치는 보안 메커니즘이 일반 컴퓨터에 비해 취약하기 때문에 특히 공격자의 표적이 되기 쉽다 [5]. 공격자가 IoT 장치를 해킹하면 위장된 신분으로 다른 정상 노드와 통신할 수 있다. 위장된 신분으로 다른 노드와 통신할 때에는 상대방의 개인정보를 사취할 수 있다.

그리고 개인정보 데이터를 네트워크에 보내는 것은 위험한 행위이다. 통신 절차에 네트워크 공격을 당하여 데이터 노출하거나 목적지가 아닌 다른 IP 주소에 전달하게 되면 개인정보가 노출된다. 그러므로 데이터 통신할 때에 어느 방식으로 민감한 데이터를 보내지 않아도 수행하고 싶은 업무를 처리할 수 있다는 기술이 필요하게 된다 [6].

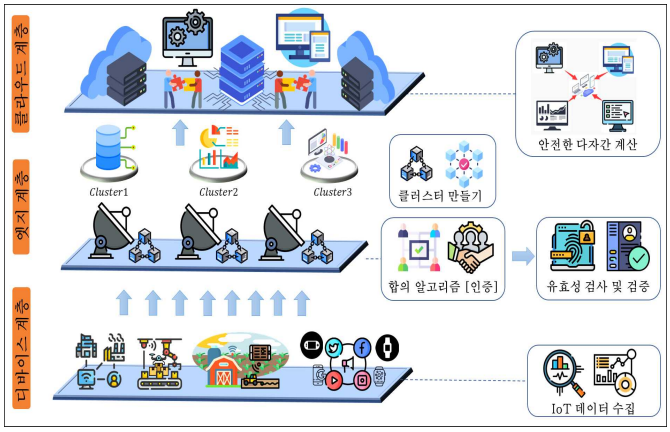
2.2. 개인정보를 보호하기 위한 기술 동향

개인정보를 보호하기 위해서는 연합 작업 중에서 데이터의 유효성 및 통신 상대방의 신분을 파악해야 한다. 블록체인은 공평하고 강력한 합의 알고리즘으로 인증 메커니즘을 제공하여 네트워크에 있는 모든 노드가 합의 알고리즘을 완성한 노드의 신분을 식별할 수 있다. 또한, 합의 알고리즘을 통과하는 노드는 분산형 네트워크에서 해당 데이터를 보낸 사실에 대해 부인할 수 없다. 만약 합의 알고리즘을 통과한 노드가 어떤 악의적인 데이터를 보내게 되면, 블록체인은 정보의 출처를 추적할 수 있으며, 노드는 책임을 전가할 수 없다.

게다가, 개인정보를 보호하기 위해서 개인정보와 비슷한 민감한 데이터는 가능한 한 네트워크에 보내지 않아야 한다. 그러므로 맹목적인 컴퓨팅 기술에 대한 필요성이 점점 심각해지고 있다. 안전한 다자간 계산은 다자간 계산할 때에 서로 자기 자신이 가지고 있는 데이터를 서로 보여주지 않은 동시에 어떤 업무를 연합 수행이 가능한 기술이다. 안전한 다자간 계산은 맹목적인 컴퓨팅을 실현할 수 있기 때문에 개인정보 문제를 해결에 우세가 존재하다.

3. 블록체인&안전한 다자간 계산 기반 IoT 네트워크 아키텍처

본 논문에서 블록체인 및 안전한 다자간 계산을 활용하는 IoT 네트워크를 제안한다. 그림1과 같게 IoT 네트워크를 디바이스 계층, 엣지 계층, 클라우드 계층으로 나눠봤다.



(그림 1) 블록체인 기반의 안전한 다자간 계산 아키텍처

그림1과 같이, 디바이스 계층의 IoT 장치들이 데이터를 수집한 후에 먼저 엣지 계층에 배치되는 블록체인 네트워크에서 인증을 받아야 한다. 인증을 받기 전에 해당 데이터를 상층 네트워크에 보낼 수 없다. 블록체인은 인증 메커니즘은 합의 알고리즘에 기반한 것이고, 합의 메커니즘을 통과해야 데이터를 네트워크에 보낼 수 있다. 합의 알고리즘은 다수적 존재하기 때문에 선택할 때에는 업무 유형에 따라서 가성비 최적화되는 알고리즘을 선택해야 한다. 예컨대, 에너지 소모가 상대적 큰 업무는 PoW 알고리즘 적합하지 않다. IoT 장치가 합의 알고리즘을 통과하자마자 해당 장치의 출처나 업무 유형, 소속기관 등 식별자를 통해서 한 클러스터에 추가한다. 앞으로 클라우드에 연합 계산이 필요한 경우에 클러스터를 기본 단위로 안전한 다자간 계산을 진행한다.

IoT 데이터가 각자의 클러스터에 모이기 때문에 추후 어떤 이유로 책임을 추궁하면 당사자가 부인할 수 없다. 이를 실현하기 위해서는 블록체인에서 만든 블록은 해당 블록을 만드는 노드의 공개키 정보가 존재해야 한다. 안전한 다자간 계산에 참여하기 전에 해당 공개키 정보를 사용하여 디지털서명을 요청하면 신분 검증이 가능하다. 디지털서명 검증 실패는 본인이 아니라는 것을 증명하게 되기 때문에 해당 조작은 무효 조작을 간주한다.

인증 메커니즘을 통한 모든 데이터들은 안전한

다자간 계산에서 사용하기 가능하다. 안전한 다자간 계산은 여러 가지 방법으로 실현이 가능하다. 핵심 요구사항은 입력값을 상대방이 보이지 않은 상태에서 어떤 방법을 통해 해당 입력 데이터를 사용하여 계산을 진행한다는 것이다. 입력값 x 및 y에 대해서 맹목적인 컴퓨팅을 구현하자면 (E는 암호화, D는 복호화), $E(x+y)=E(x)\times E(y), x,y\in K$에 만족해야 한다. 암호학적으로 분석해보면, 원래는 "x+y"에 대한 계산은 각자의 입력값을 암호화하여 E(x), E(y)를 얻은 후에, 암호문을 교환하여 E(x)*E(y)를 계산하면 된다. 복호화인 경우에서 모든 참가자에게는 D(E(x)*E(y))로 원하는 연합 계산 결과를 얻을 수 있다. 그럼 입력값은 서로 보이지 않은 동시에 원하는 업무를 연합 계산할 수 있는 상태라서 맹목적인 컴퓨팅으로 안전한 다자간 계산을 실현할 수 있다.

4. 기밀성의 수학적 증명

Paillier 암호는 덧셈 동형 성질을 가지고 있는 비대칭암호라서 안전한 다자간 계산의 알고리즘으로 구축할 수 있다. Paillier 암호 기반 안전한 다자간 계산은 키 생성 단계, 암호화 단계, 복호화 단계 3가지 단계로 구성되어 있다.

키 생성 단계: 매우 큰 소수 p 및 q를 선택하여 $n=p\cdot q$ 및 $\lambda=\mathrm{lcm}(p-1,q-1)$를 계산한다. lcm은 최소공백수의 계산공식이며, λ는 개인키이다.

암호화 단계: 명문 m에 대해서 난수 r를 생성하고 나서 암호문 $c=g^m\cdot r^n \bmod n^2$를 계산한다. g는 mod n^2의 생성원이다. 생성원은 군의 주어진 부분집합을 포함하는 최소의 군을 생성부분군이라 한다.

복호화 단계: 암호문 c에 대해서 $m=L(c^\lambda \bmod n^2)*\mu \bmod n$으로 계산할 수 있으며, 그 중에서 $L(x)=\frac{x-1}{n}, \mu=(L(g^\lambda \bmod n^2))^{-1}$.

Paillier 암호 기반의 덧셈 동형 성질은 다음과 같이 증명할 수 있다.

$$c_1\cdot c_2 \bmod n^2=(g^{m_1}\cdot r_1^n)(g^{m_2}\cdot r_2^n) \bmod n^2$$
$$=g^{m_1+m_2}(r_1\cdot r_2)^n$$

안전한 다자간 계산을 진행할 때 참가자는 먼저 공개키 및 개인키를 선택하고, 각자 명문 m에 대해서 암호화하여 각자의 암호문 c를 얻는다. 그 다음에 각자의 c를 교환하여 $c_1\cdot c_2 \bmod n^2$를 계산한다. 그리고 개인키로 해당 암호문을 해독하고 나서 명문 m_1+m_2를 얻을 수 있다. 그 과정에서는 참가자가 각자의 입력 정보 m에 대한 정보가 다른 참가자에게 노출하지 않고, 각자만 보유하게 된다.

5. 결론 및 고찰

개인정보가 IoT 네트워크에서 네트워크 공격이나 악의적인 유도 때문에 정보 노출이 되어서 큰 위험이 직면하고 있다. 본 논문에서 블록체인으로 인증하여 유효한 데이터를 클러스터로 만든 후에 유효한 데이터만 이용한 IoT 네트워크 아키텍처를 제안한다. 통신 절차에서 인증된 클러스터가 식별자로 데이터의 소스 주소를 파악할 수 있다. 그리고 민감하거나 기밀성 요구된 다자간 데이터 교환를 요구한 업무를 처리하려면 안전한 다자간 계산을 이용하여 서로 개인정보를 보호할 수 있다. 안전한 다자간 계산 기반한 IoT 네트워크 구조는 암호학 기술을 활용하기 때문에 암호학 발전에 따라서 지속적으로 발전 가능하며 다른 기술과 연동하여 사용하는 잠재력이 있다.

본 논문에서의 개선할 수 있는 점을 간략히 살펴보면 안전한 다자간 계산 실현 가능한 알고리즘에 개발하거나 블록체인 차원에서 IoT 네트워크 및 스마트 장치들에 대한 적합한 아키텍처를 재설계할 것이다. IoT 영역의 블록체인 응용 및 맹목적인 컴퓨팅 기술의 발전에 가이드라인 제시한다.

사사

This research was supported by the National Research Foundation of Korea(NRF) funded by the Ministry of Science and ICT. (RS-2023-00267476)

참고문헌

[1] Park J. S. and Park J. H., "Future Trends of IoT, 5G Mobile Networks, and AI: Challenges, Opportunities, and Solutions," JIPS, vol. 16, no. 4, pp. 743-749. (2020).

[2] Salim, M. M., Shanmuganathan, V., Loia, V., & Park, J. H., "Deep Learning Enabled Secure IoT Handover Authentication for Blockchain Networks.", HCIS, (2021).

[3] Monrat, Ahmed Afif, Olov Schelén, and Karl Andersson. "A survey of blockchain from the perspectives of applications, challenges, and opportunities." IEEE Access 7 (2019):

117134-117151.
[4] Du, Wenliang, and Mikhail J. Atallah. "Secure multi-party computation problems and their applications: a review and open problems." Proceedings of the 2001 workshop on New security paradigms. (2001) .
[5] Liu Zhicheng, "A new theory on the construction of Internet of Things Network information security ecosystem." Cyberspace Security vol. 9, pp. 12, (2020).
[6] Wu hongying, "Research on privacy data security for Internet of Things." Wireless Internet Technology, vol. 17, No. 8, pp. 21-22. (2020).